THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF APPEALS

In Re Application of:)
) ATTORNEY FILE NO.:
Inventors: Sridhar Dathathraya) SLA1055
)
Serial No.: 09/944,695)
) Examiner: Ha, Leynna
)
Filed: August 31, 2001) Customer No.: 55,286
)
Title: SYSTEM AND METHOD FOR) Group Art: 2135
SECURE COMMUNICATIONS)
WITH NETWORK PRINTERS) Confirmation No.: 2135
)

CERTIFICATION UNDER 37 CFR § 1.8

I hereby certify that this correspondence is being facsimile transmitted to the US Patent and Trademark Office, fax No. 571 273 8300, on this date 5/15/2006.

Date 5/15/2006 Signature

Hon. Commissioner Of Patents And Trademarks
Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

REPLY BRIEF ON APPEAL

This is a Reply Brief responsive to an Examiner's Answer dated May 5, 2006. At issue is the rejection by Examiner Leynna Ha, Group Art Unit 2135, of claims 1-8, 10-25, and 27-35, all claims in the application.

An Examiner's Answer was previously filed on December 30, 2005. The Applicant filed a Reply Brief on January 19, 2006. However, the Examiner's Answer was returned to the Examiner as undocketed on April

24, 2006. Therefore, the instant Reply Brief is responsive to the Answer of May 5, 2006.

The Applicant respectfully submits that the Examiner's analysis of the Mazzagatte is inaccurate. In summary, the Mazzagatte disclosure describes a printer that receives documents from a source, such as a PC, encrypts the documents, and stores the documents (in a server or memory). Later, when the document is to printed, the encrypted document is retrieved, decrypted, and printed. This procedure is shown in Fig. 5 and described at col. 7, ln. 45, through col. 9, ln. 34.

Mazzagatte states that the PC preferably sends the document to the printer using TCT/IP or SSL protocol. In a single line, Mazzagatte states that the document may be "encrypted" (col. 8, ln. 12-16) prior to transmission to the printer. A significant portion of the Examiner's Answer suggests that Mazzagatte uses Public key, Private keys, or Symmetric keys in encrypting the document at the PC, prior to it being sent to the printer. However, this analysis is not accurate. For example, page 21 of the Examiner's Answer (the last four lines of the page) states that, "Mazzagatte discloses encrypting data prior to transmitting to the receiving networked connected printer using Public Key infrastructure, symmetric, or asymmetric key infrastructure (col. 8, lines 38-40 and col. 9, lines 15-16)."

Col. 8, ln. 35-43, actually discusses the use of a Public Key as a form of personal identity as follows:

> The smart-card could contain the recipient's unique identification information in digital form which is supplied to the computer through smart-card interface 265. Alternatively, the information may be obtained from a digital certificate, obtained via a Public Key Infrastructure, over the internet, by e-mail or some other means. In this case, the

information could be downloaded to computer 10 over the internet to be subsequently submitted with the print job.

While the association of a print job with a personal ID is a form of security, this cited passage clearly does not state that documents are sent from a source computer to a printer encrypted using some kind of key.

Col. 9, ln. 7-24, describes the encryption performed at the printer after a document is received from the PC, as follows:

> Upon receiving the data, the print node then processes the print data and digital certificate to securely store the print data. In step S504, the print node generates a unique symmetric key utilizing a symmetric encryption algorithm. The print node encrypts the print data with the symmetric key in step S505, encrypts the symmetric key with the public key of the print node, and stores the encrypted print data, either locally or remotely. Although the present invention is described as preferably utilizing a symmetric key, an asymmetric key, such as a public/private key pair, may also be utilized in the same manner as the symmetric key. It should also be noted that in a case where the print node is a printer, the print node uses the printer's public key to encrypt the symmetric key. However, in a case where the print node is a gateway to multiple printers, the print node uses the public key of the gateway to encrypt the symmetric key. The reasons for this distinction will be described in more detail below.

The above-cited passage clearly describes encryption performed at the printer, after the document has been received from a source computer.

Besides the inaccurate representation of the Mazzagatte disclosure, the Examiner's Answer still fails to make a *prima facie* argument that the combination of the Mazzagatte and DeBry references makes the claimed limitations obvious. At the bottom of page 23 of the Answer it states, "(t)herefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Mazzagatte with DeBry for receiving an encrypted document with a public key and a private key is used for decrypting at the printer because public/private key cryptography presents unauthorized printing and spoofing.". In response, the Applicant notes that while cryptography may prevent unauthorized printing, this statement is hardy proof that an expert would have found it obvious to combine the prior art. Further, this statement is not proof that such a combination suggests a procedure that prevents anyone but the user (who sends the document to the printer), from decrypting and printing a document at a printer.

The motivation to combine references should not be based on the conclusory statement that it would have been obvious to combine references to achieve some desirable outcome. This type of analysis is retrospective, based upon the Applicant's invention, not the references. That is, the above-quoted statement uses the Applicant's invention as the goal, and pulls the parts needed to accomplish the goal from the prior art references. Such a retrospective analysis would permit any two references to be combined merely as the result of a key word search.

As noted in the Appeal Brief, the differences between the prior and the claimed invention at first glance appear subtle, but point to different, and conflicting uses for cryptography. Mazzagatte discloses a printer that stores and retrieves encrypted documents. DeBry describes the use of encryption to protect the file source (i.e., a third party). The Applicant does not see how these references can be combined, as these two disclosures are using cryptography to protect different (contradictory) interests. However, even if DeBry is combined with Mazzagatte, the combination does not suggest that Mazzagatte can be modified in such a manner as to give the user control of the document decryption key. Alternately stated, neither DeBry nor Mazzagatte describe the claimed invention process, which primarily protects the security of the user (document sender), not the security of a printer, a server, or a third party.

In summary, the Applicant's claimed invention does not simply recite the use of a key to encrypt documents. Rather, the novelty is in the limitation of the user (the person sending the document to the printer) retaining control over the encryption key. The claimed invention makes it absolutely impossible for anyone but the document sender to print a document by "spoofing" the printer, because only the document sender controls the key.

It is submitted that the claims in the present application clearly and patentably distinguish over the cited references. Accordingly, the Examiner should be reversed and ordered to pass the case to issue.

Respectfully submitted,

Date: 5/15/2006

Gerald Maliszewski
Registration No. 38,054

Customer Number 55,286
P.O. Box 270829
San Diego, CA 92198-2829
Telephone: (858) 451-9950
Facsimile: (858) 451-9869
gerry@ipatentit.net